GP 2766

#7

Pre Amdt

Docket No. 0225-4188

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Lenstra et al.		
Serial No.:	09/498,716	Group Art Unit:	Unassigned
Filed:	February 7, 2000	Examiner:	Unassigned
For:	EFFICIENT AND COMPACT SUBGROUP TRACE REPRESENTATION ("XTR")		

PRELIMINARY AMENDMENT

Honorable Assistant Commissioner
of Patents and Trademarks
Washington, D.C. 20231
Sir:

Prior to examination on the merits, please Amend the above-identified application as follows:

IN THE SPECIFICATION

Please enter the changes to the specification as indicated on the attached AMENDED SPECIFICATION. The amended specification is a marked up copy with the insertions underlined and deletions bracketed. All changes are highlighted on the document for clarity.

IN THE ABSTRACT

Please delete the current Abstract in its entirety and insert the following:

N.E.

--The invention is a method, system, computer program, computer program article of manufacture, and business method for providing improvements in key generation and cryptographic applications in public key cryptography, by both reducing: 1) the bit-length of public keys and other messages, thereby reducing the bandwidth requirements of telecommunications devices, such as wireless telephone sets, and 2) the computational effort required to generate keys, to encrypt/decrypt and the generate/verify digital signatures. The method of the invention determines a public key having a reduced length and a factor p, using GF(p^2) arithmetic to achieve GF(p^6) security, without explicitly constructing GF(p^6).--